

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

5/11/2010

**SUBJECT:**

Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (MS10-031).

**OVERVIEW:**

A vulnerability has been discovered in Microsoft Visual Basic for Applications (VBA). VBA is used for developing client desktop packaged applications and integrating them with existing data and systems. Exploitation may occur if a user opens a specially crafted file which supports VBA and can be exploited via email or through the Web. This can be a Word document, an Excel spreadsheet, a PowerPoint presentation or any other type of document that uses VBA. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**SYSTEMS AFFECTED:**

Microsoft Office XP  
Microsoft Office 2003  
Microsoft Office 2007  
Third Party Applications that use Microsoft Visual Basic for Applications  
Microsoft Visual Basic for Applications 6.x  
Microsoft Visual Basic for Applications SDK 6.x

**RISK:****Government:**

Large and medium government entities: **High**  
Small government entities: **High**

**Businesses:**

Large and medium business entities: **High**  
Small business entities: **High**

**Home users: High**

**DESCRIPTION:**

A vulnerability exists in Microsoft Visual Basic for Applications (VBA) that could allow an attacker to execute arbitrary code on an affected system. This remote code execution vulnerability is due to the way VBA searches for ActiveX controls. This vulnerability can be triggered by opening a specially crafted file and can be exploited via email or through the Web. In the email base scenario, the user would have to open the specially crafted file as an email attachment. In the Web based scenario, a user would have to open a specially crafted file that is hosted on a malicious web site. Successful exploitation may result in an attacker gaining the

same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Please note that Microsoft has indicated that there are known issues when implementing this update. Microsoft Knowledge Base Article 978213 (<http://support.microsoft.com/kb/978213>) outlines the known issues and solutions for these issues.

It should be noted that by default, Microsoft Office 2007 prompts a user with a security warning before activating an embedded ActiveX control in an Office document. Users who choose to not enable the control are protected by this default setting. For more information, see the following Microsoft Office Online article: <http://office.microsoft.com/en-us/help/HA100310671033.aspx>

## **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to download files from un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- If the patch cannot be applied, consider the following workarounds
  - Disable ActiveX controls within the 2007 Microsoft Office System.
  - Restrict access to 'VBE6.dll' by using an Access Control List (ACL).
  - Use the Microsoft Office Isolated Conversion Environment (MOICE) when opening files received from untrusted or unknown sources.

## **REFERENCES:**

### **Microsoft:**

<http://www.microsoft.com/technet/security/bulletin/ms10-031.msp>  
<http://support.microsoft.com/kb/978213>  
<http://blogs.technet.com/msrc/archive/2010/05/11/may-2010-security-bulletin-release.aspx>

### **Secunia:**

<http://secunia.com/advisories/39663>

### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0815>